IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
NEWNAN DIVISION

UNITED STATES OF AMERICA	:	
	:	
v.	:	Criminal Action No.
	:	3:21-CR-0004-TCB-RGV
ROBERT PURBECK	:	

MOTION TO SUPPRESS EMAIL SEARCHES AND TO SUPPRESS ITEMS COVERED BY SEARCH WARRANT NO.: 1:21-MC-1981

Defendant Robert Purbeck hereby respectfully moves to suppress any and all evidence, information, or other matters arising from (1) the illegal searches and seizures that the government conducted on his email accounts, and (2) the illegal searches of various devices described in Search Warrant No. 1:21-MC-1981 (NDGA).

I. THE SEARCHES OF MR. PURBECK'S EMAIL ACCOUNTS

From what Mr. Purbeck has been able to determine, the government obtained copies of the following email accounts independent of the government's conduct on August 21, 2019 in Idaho using various court-issued orders or warrants:

(1) email account for rpurbeck@gmail.com from Google pursuant to July, 2019 §2703(d) Order from this Court (search warrant and application filed under seal as Exhibit L); and referred to hereafter as the "§2703(d) Order:"

(2) email account for rpurbeck@gmail.com from Apple pursuant to August, 2019 search warrant from this Court (different judge) (search warrant and application filed under seal as Exhibit M; referred to hereafter as the "Apple Search Warrant;"

(3) email account for jrjboise82@aol.com from Oath pursuant to August 2019 search warrant from this Court (search warrant and application filed under seal as Exhibit N); referred to hereafter as the "Oath Search Warrant" and

(4) email account for rpurbeck1@gmail.com from Google pursuant to August 2019 search warrant from this Court (search warrant and application filed under seal as Exhibit O); referred to hereafter as the "Google Search Warrant."

Each of these searches appear to be based on search warrants from this Court, although issued by different Judges than the Judges assigned to this case. These are all Mr. Purbeck's email addresses in which he has a right to privacy and a right against unwarranted and unreasonable government intrusion. See, e.g., United States v. Wilson, 13 Fed. 4th 961, 967 (2021). Mr. Purbeck challenges as illegal all of the searches and seizures related to his email accounts.

A. The United States District Court for the Northern District of Georgia Lacked Jurisdiction to Issue the Orders and Warrants to Search and Seize Mr. Purbeck's email accounts

Under Federal Rule of Criminal Procedure 41, a court can issue a "warrant to search for and seize a person or property located within the district." Fed. R.

Crim. P. 41(b)(1). None of Mr. Purbeck's email account providers are within the Northern District of Georgia. They are not even in the State of Georgia. So, even though the search warrants reference "the property described" as being "in the Northern District of Georgia," that is not accurate. (See Exhibits M, N, and O). It is undisputed that none of Mr. Purbeck's email account records are within the Northern District of Georgia; indeed, they are not even within the State of Georgia. Accordingly, Rule 41(b)(1) does not provide a basis to issue a search warrant for Mr. Purbeck's email accounts. As best as Mr. Purbeck can determine, none of the other provisions under the portion of Rule 41 titled "Venue for a Warrant Application" authorize this Court to issue a warrant for Mr. Purbeck's email account records. See Fed. R. Crim. P. 41(b)(2)-(6).

Some courts have held that, because Rule 41 specifically states that it does not "modify any statute regulating search or seizure," courts are authorized to issue search warrants under 18 U.S.C. §2703 without regard to the venue provisions of Rule 41. See In re Search Warrant, No. 6:05-MC-168-Orl-31JGG, 2005 WL 3844032, at *5-6 (M.D. Fla.) ("Section 2703(a) permits a district court to issue out-of-district warrants" without regard to the Rule 41 venue provisions provided that the issuing court is where the crime occurred). Under 18 U.S.C. §2703(d), a court can issue an order for a person's email records if it is a "court of competent jurisdiction," which is defined, among other ways, as a district court that has

"jurisdiction over the offense being investigated." 18 U.S.C.A. § 2711(3)(A)(i). This is a territorial limitation on the power of courts to issue orders and warrants under §2703. See In re Search Warrant, No. 6:05-MC-168-Orl-31JGG, 2005 WL 3844032, at *5-6 (M.D. Fla.).

With respect to the §2703(d) Order for Mr. Purbeck's gmail account from Google and with respect to the three search warrants for Mr. Purbeck's various email accounts, this Court lacked jurisdiction to issue this order or these warrants because it was not a district court that had jurisdiction over the offense being investigated as to Mr. Purbeck in July/August, 2019 when seeking these orders and warrants. Here is why.

First, with the respect to the §2703(d) Order, there are two allegations of crimes in the application: (1) an extortion email from someone called "Lifelock" related to a healthcare provider in California, and (2) a general conclusory allegation that Lifelock sold stolen personal financial and identification information on the internet through a marketplace called AlphaBay, which allegedly is a darknet marketplace. Neither of those allegations regarding crimes say anything about Georgia, much less the Northern District of Georgia.

Indeed, the only reference to the Northern District of Georgia is in paragraph 11 of the application when it says that Bitpay, an Atlanta-based bitcoin payment processor, processed some bitcoin transactions from "Studmaster 1" – a different

account from Lifelock, but one that law enforcement alleged was controlled by the same person as Lifelock. Nothing about the Studmaster1 bitcoin transactions with Bitpay are alleged to have been illegal. There is no allegation that any bitcoin transactions involving Studmaster1 and Bitpay (the Atlanta connection) are illegal. Therefore, based on the application for the §2703(d) Order, it is impossible for this Court to have jurisdiction over any crime involving Mr. Purbeck such that it would be a court of competent jurisdiction for purposes of issuing a §2703(d) Order for Mr. Purbeck's rpurbeck@gmail.com account with Google.

A similar, but slightly different problem, exists with the three search warrants that were issued for Mr. Purbeck's various email accounts. According to the search warrant applications, "Lifelock" (who allegedly is actually Mr. Purbeck acting under the alias "Lifelock") is alleged to have sent extortion emails to three victims: one in California, one in Michigan, and one in Massachusetts. (See Apple Warrant application at ¶¶ 14-17; Oath Warrant application at ¶¶ 15-18; Google Warrant application at ¶¶ 15-18). Once again, Lifelock is not alleged to have committed any crimes against anyone in Georgia, much less in this district. The Bitpay transactions are alleged again, but this time there is no mention that Bitpay is an Atlanta-based (or Georgia-based) entity, or otherwise has any ties to this district. And, as before, there were no allegations that any of these Bitpay transactions were criminal in nature.

The way in which the government appears to be tying Lifelock to Georgia is through earlier paragraphs in which the search warrant affidavit alleges that "TDO, a hacker group also known as "thedarkoverlord," includes Lifelock within its membership. (See Apple Warrant application at ¶¶ 7-13; Oath Warrant application at ¶¶ 8-14; Google Warrant application at ¶¶ 8-14). Lifelock is not alleged to have committed any offenses in Georgia, either individually or through TDO. Rather, TDO is alleged to have stolen healthcare provider information "from an unidentified health care provider in Georgia" (but not necessarily in the Northern District of Georgia) and, thereafter, law enforcement while located in the Northern District of Georgia purchased some of these stolen healthcare records. (See Apple Warrant application at ¶ 12; Oath Warrant application at ¶ 13; Google Warrant application at ¶13). There is no allegation that Lifelock (or Mr. Purbeck under any variation) stole these records from the Georgia healthcare provider or sold any of these Georgia records to the law enforcement agents who were sitting in the Northern District of Georgia.

Rather, it appears that the government is contending that Lifelock is associated with TDO via allegations of similarities in their criminal schemes and "the claim by Lifelock to be TDO," which follows a lengthy redaction and puts Mr. Purbeck in an impossible position to address in this motion. (See, e.g., Apple Warrant application at ¶¶ 23-26; Oath Warrant application at ¶¶ 24-27; Google

Warrant application at ¶¶ 24-27). Mr. Purbeck did have an exchange with an on-line entity in which he first said he was part of TDO and then promptly announced he was not part of TDO, once he had looked up TDO and found out who they were. (See Exhibit A, at ¶29). In fact, Mr. Purbeck is not and never has been part of TDO. (See id.). If this is the conversation that is redacted and that the government was referring to in the search warrant applications, then the government should have provided the full conversation to the Court, and not selective tid-bits, if that is what happened, which again Mr. Purbeck cannot effectively address given the redactions in the search warrant application.

With respect to the allegations that Lifelock and TDO operate in a similar fashion, the details of these similarities are quite generic and do not constitute any sort of modus operandi. (See Apple Warrant application at ¶23; Oath Warrant application at ¶24; Google Warrant application at ¶24). In fact, they represent, at least based on the unredacted portions of the search warrant affidavit, conclusory allegations without any facts from which the Court could assess the accuracy or reliability of these law enforcement conclusions. An affidavit lacks the sufficient indicia of probable cause when it is a bare-bones statement with only conclusory allegations. See United States v. Gonzalez, 1:09-CR-00371-TWT-AJB, 2010 WL 2721882 (N.D. Ga. May 25, 2010) report and recommendation adopted, 1:09-CR-371-TWT, 2010 WL 2721540 (N.D. Ga. July 7, 2010); United States v. Lebowitz,

647 F.Supp.2d 1336, 1355 (N.D.Ga.2009) (Story, J., adopting King, M.J.) (citing United States v. Glinton, 154 F.3d 1245, 1257 (11th Cir.1998)); see also United States v. Laughton, 409 F.3d 744, 745 (6th Cir.2005) (labeling affidavits lacking indicia of probable cause as " 'bare bones' affidavits" and indicating that such affidavits only contain "suspicions, beliefs, or conclusions, without providing some underlying factual circumstances regarding veracity, reliability, and basis of knowledge") (citation omitted). Accordingly, those conclusory allegations are not sufficient to provide probable cause that Mr. Purbeck had any possible association with TDO or TDO's actions in Georgia, such that this Court would have jurisdiction over any of the crimes alleged in the warrant applications.

Without this Court being a court having jurisdiction over the offenses alleged against Mr. Purbeck in the search warrant applications at the time the search warrants were issued, this Court was without jurisdiction to issue those warrants under Rule 41 of the Federal Rules of Criminal Procedure or 18 U.S.C. §2703. Accordingly, all of the following are void orders or warrants for lack of jurisdiction of the issuing court: (1) the July, 2019 2703(d) Order from this Court for the email account rpurbeck@gmail.com from Google, (2) the August, 2019 search warrant from this Court for the email account for rpurbeck@gmail.com, (3) the August 2019 search warrant from this Court for the email account for jrjboise82@aol.com from Oath, and (4) the August 2019 search warrant from this

Court for the email account for rpurbeck1@gmail.com from Google. The Court should suppress any and all evidence obtained from or as a result of these orders and warrant and the Court should further suppress any fruits of the poisonous tree of these illegal searches and seizures.

B. Redacted Search Warrant Applications and Need for Full Unredacted Applications

At present, the government has only provided Mr. Purbeck with a redacted copy of the search warrant applications. Mr. Purbeck has requested the full unredacted copy of the warrant applications, and the government has refused to produce them. Without the full unredacted warrant applications, Mr. Purbeck cannot determine all of the arguments or grounds that he may have to contest the legality of the warrant to search his home. Mr. Purbeck has moved to compel the government's failure to provide full unredacted copies of the warrant applications, and he further respectfully requests and reserves the right to amend and supplement any and all grounds to challenge these orders and warrants until after unredacted copies of the applications have been produced and he has had an opportunity to review them in context of the voluminous discovery in this case. Subject to receiving the unredacted search warrant and §2703(d) applications and based on what Mr. Purbeck has been able to review at present, Mr. Purbeck raises

the following grounds to challenge the legality of the warrants to search and seize his email accounts.

C. The §2703(d) Order was not founded on Probable Cause as Required

Under 18 U.S.C. §2703(d), the government must simply offer "specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation." 18 U.S.C. 2703(d). That is what happened with the July, 2019 Order from this Court for Mr. Purbeck's email account with Google: the Court found that "reasonable grounds to believe" existed. The Court did not find probable cause. And yet, the government, using this Court's power, was able to obtain large amounts of information from Mr. Purbeck's email account, all without any sort of date limitation.

Mr. Purbeck's email account information and the §2703(d) Order in this case is much more akin to the cell phone data that the United States Supreme Court found in Carpenter v. United States, 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018) required probable cause before the government could obtain that information than the common cell tower dump that this Court (and other courts) has held does not require a showing of probable cause. See, e.g., United States v. Manning, No. 119CR00376TWTRGV, 2021 WL 5236660, at *6 (N.D. Ga. Aug. 20,

2021), report and recommendation adopted sub nom. United States v. Davis, No. 1:19-CR-376-4-TWT, 2021 WL 5232480 (N.D. Ga. Nov. 10, 2021) (citing United States v. Rhodes, CASE NO. 1:19-CR-0073-AT-LTW, 2020 WL 9461131, at *3 (N.D. Ga. June 18, 2020), adopted by 2021 WL 1541050, at *2 (N.D. Ga. Apr. 20, 2021)). Mr. Purbeck respectfully submits (1) that probable cause is the standard that should have governed the §2703(d) request for his email account records, and (2) that there was no probable cause to sustain the issuance of an order to obtain his email records.

D. The Search Warrants Were Based on Illegally-Obtained Information and/or Information Excludable under *Franks*

Evidence seized as the result of an illegal search may not be used by the government in a subsequent criminal prosecution. Franks v. Delaware, 438 U.S. 154, 171 (1978). The exclusionary rule is "a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect." United States v. Calandra, 414 U.S. 338, 348 (1974). "Probable cause to support a search warrant exists when the totality of the circumstances allows the conclusion that "there is a fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983). This Court's duty in reviewing the challenged search warrant is "simply to ensure that the [judge

issuing the warrant] had a substantial basis for concluding that probable cause existed." Id.

To establish probable cause, an affidavit submitted to obtain a search warrant must state facts that are "sufficient to justify a conclusion that evidence or contraband will probably be found at the premises to be searched." United States v. Martin, 297 F.3d 1308, 1314 (11th Cir. 2002). The affidavit must "establish a connection between the defendant and the [location to be searched] and a link between the [location to be searched] and any criminal activity." Id. A bare-bones affidavit that contains nothing more than conclusory allegations is insufficient to establish probable cause. Id. at 1313-1314. "Intentional or reckless omissions by an affiant in a search warrant will invalidate a warrant 'only if inclusion of the omitted facts would have prevented a finding of probable cause.'" United States v. Brown, 370 Fed. Appx. 18, 21 (11th Cir. 2010) (quoting Madiwale v. Savaiko, 117 F.3d 1321, 1327 (11th Cir. 1997)).

1. Paragraph 19 of the Apple Warrant Applications and Paragraph 20 of the Oath and Google Warrants Applications

These paragraphs of the Warrant Applications refer to email/direct messages that the government obtained from Alphabay. These messages were Mr. Purbeck's private messages, and he has a right against government intrusion as to those email/direct messages, as well as other private communications on this platform.

See, e.g., United States v. Wilson, 13 Fed. 4th 961, 967 (2021). As far as Mr. Purbeck has been able to determine, the government did not obtain a search warrant to access and read Mr. Purbeck's private email/direct messages that were held on the Alphabay servers/company records. The government seizures and searches of Mr. Purbeck's emails/messages violates the Fourth Amendment proscription against unreasonable and warrantless seizures and searches. See, e.g., Wilson, 13 Fed. 4th at 967. Accordingly, these paragraphs should be stricken from all three Warrant Applications.

2. Paragraph 33 of the Apple Warrant Applications and Paragraph 34 of the Oath and Google Warrants Applications

These paragraphs of the Warrant Applications refer to a "private message" sent by Mr. Purbeck on the Alphabay platform. The government has not produced and, as far as Mr. Purbeck has been able to determine, the government does not have a search warrant that authorizes the government to seize or search or read Mr. Purbeck's emails/communications transmitted through the Alphabay platform. The government's seizures and searches of Mr. Purbeck's emails/messages violates the Fourth Amendment proscription against unreasonable and warrantless seizures and searches. See, e.g., Wilson, 13 Fed. 4th at 967. Accordingly, these paragraphs should be stricken from the Warrant Applications.

3. Paragraphs 48 - 50 of the Apple Warrant Application and Paragraphs 49 - 51 of the Oath and Google Warrant Applications

In these paragraphs of the respective Warrant Applications, the affidavit refers first to IP address 24.117.83.148 and then to IP address 24.117.84.148. This latter IP address returns to Sioux City, Iowa, which is nowhere near Meridian, Idaho. (See Exhibit J). Accordingly, the statement "IP address 24.117.84.148 provides service to the Meridian, Idaho area" is false. It also makes the references to this IP address irrelevant as to Mr. Purbeck and his email accounts, as he clearly lives in Meridian, Idaho. What is unclear at this point is whether the interchanging use of these two different IP addresses is simply a scrivener's error, thereby making this statement false, but negligently so, which would preclude a challenge under Franks, or an intentional (or at least reckless) false statement, making a challenge under Franks appropriate.

4. Paragraphs 50 - 56 of the Apple Warrant Application and Paragraphs 51 - 57 of the Oath and Google Warrant Applications

These paragraphs in the respective warrant applications are all directly derived from the §2703(d) Order for Mr. Purbeck's email account rpurbeck@gmail.com from Google. Mr. Purbeck has challenged the legality of that §2703(d) Order, above. To the extent the Court grants Mr. Purbeck's motion and finds the §2703(d) Order is void or illegal, then these paragraphs should all be

removed from the warrant applications for Apple, Oath, and Google, and the Court should re-assess probable cause without the offending paragraphs.

II. SEARCHES UNDER SEARCH WARRANT NO. 1:21-MC-1981

Mr. Purbeck also challenges as illegal searches and seizures of the devices covered under Search Warrant No. 1:21-MC-1981 (NDGA), which authorized the government to search a CD and various thumb drives, as described in that warrant. (See Exhibit P). Mr. Purbeck's challenge to these searches and seizures is based on the following which will be dependent on how the Court rules on his other motions.

First, the entire affidavit in support of probable cause is premised on information that was gained as a result of earlier searches and seizures that Mr. Purbeck has challenged as illegal. (See Exhibit P, ¶¶ 6-20). If the Court grants his motions on those earlier items, then the corresponding portions of the search warrant affidavit for Search Warrant No. 1:21-MC-1981 will have to be removed from the probable cause analysis. Specifically, and at a minimum, paragraphs 6 through 20 of the affidavit in support of Search Warrant No. 1:21-MC-1981 will have to be excluded, depending of course on how the Court ultimately rules on Mr. Purbeck's other motions. Once that is done, no probable cause will exist; indeed, the entire "Probable Cause" section from the affidavit will have been excluded.

Second, the government's possession of the items covered by Search Warrant No. 1:21-MC-1981 are the fruits of the poisonous tree from the government's earlier searches because, but for those earlier illegalities, the government would not have possession of the items covered by Search Warrant No. 1:21-MC-1981. Accordingly, and again depending on how the Court rules on Mr. Purbeck's other motions, the devices covered by Search Warrant No. 1:21-MC-1981 should also be suppressed as the fruit of the poisonous tree of earlier illegalities.

For the foregoing reasons, and as will be more fully articulated depending on how the Court rules on Mr. Purbeck's other motions, Mr. Purbeck respectfully challenges the searches and seizures of the devices covered by Search Warrant No. 1:21-MC-1981 and all evidence and other information arising therefrom.

WHEREFORE, Mr. Purbeck respectfully requests that the Court (1) hold an evidentiary hearing on all matters raised in his motion to suppress and any others that may be developed at the hearing, (2) establish a briefing schedule for all parties to address the issues raised in this motion to suppress and developed at the evidentiary hearing, and (3) thereafter grant this motion and suppress and exclude from evidence any and all information, material, items, or evidence gathered from the illegal detentions, searches, seizures and interrogations detailed in this motion.

Respectfully submitted, this 13th day of December, 2021.

/s/ *Andrew C. Hall*
Andrew C. Hall
Georgia Bar No. 318025
Hall Hirsh Hughes, LLC
150 E. Ponce de Leon Ave., Suite 450
Decatur, Georgia 30030
404/638-5880 (tel.)
404/638-5879 (fax)
andrew@h3-law.com
Counsel for Defendant Robert Purbeck

CERTIFICATE OF COMPLIANCE WITH TYPE AND FONT

AND CERTIFICATE OF SERVICE

I hereby certify that this motion has been prepared in Courier New font (13 pt.) and consistent with the Local Rules of this Court.

I further hereby certify that I have this date caused a true and correct copy of the foregoing MOTION TO SUPPRESS EMAIL SEARCHES
AND TO SUPPRESS ITEMS COVERED BY SEARCH WARRANT NO.: 1:21-MC-1981 to be served by filing it with the Clerk of Court using the ECF System that will send notification of such filing to:

Assistant United States Attorney Michael Herskowitz and Nathan Kitchens

This the 13th day of December, 2021.

/s/ Andrew C. Hall
Andrew C. Hall